Indian Research Review

www.irrjournal.com Volume 3, Issue 4 ,ISSN : 0975-7430

Survey on active and passive attacks in Dynamic Mobile Ad-Hoc Networks

[1]Karthikeyan.U
Research Scholar ,Dept of CSE
Bharath University

[2]Dr.Rajani
Research Director,
Bharath University

Abstract

The infra-structureless nature of ad hoc networks requires the distribution of network functions to all the participating nodes. The underlying requirement for making operational the cooperative paradigm is the supposed goodbehavior of all entities composing and, at the same time, using the system. However, the lack of any centralized authority that enforces the overall collaboration motivates a possible tendency of entities toward self-interested behaviour. Ad hoc networks are distributed systems composed of autonomous entities, which need cooperation in order to work properly. The underlying concept is the exploitation of synergy, resulting from collaboration among the network components, to provide services to each other. Synergy makes up for the lack of a network infrastructure: users' devices take over infrastructural tasks like routing and forwarding in order to ensure the network's functioning. . Besides the general security objectives like authentication, confidentiality, integrity, availability and non- repudiation, the ad hoc routing protocols should also address location confidentiality, cooperation fairness and absence of traffic diversion. In this paper we attempt to analyze threats faced by the ad hoc network environment and provide a classification of the various security mechanisms. We analyzed the respective strengths and vulnerabilities of the existing routing protocols and suggest a broad and comprehensive framework that can provide a tangible solution.

Keywords:
Ad hoc networks, security attacks, secure routing

Introduction

Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. There is no fixed Infrastructure such as base stations for mobile switching. Nodes within each other's radio range communicate directly via wireless links

which are far apart rely on other nodes to relay messages. Node mobility causes frequent changes in topology. The wireless nature of communication and lack of any security infrastructure raises several security problems [1] [2]. The following flowchart depicts the working of any general ad-hoc network.

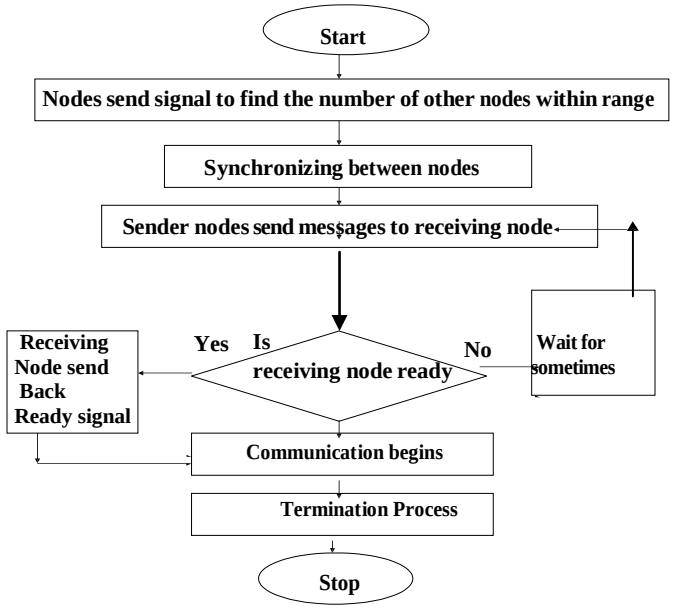

Figure 1: Working of a general Ad-Hoc Network

There are two different types of wireless networks:

- The easiest network topology is where each node is able to reach all the other nodes with a traditional radio relay system with a big range. There is no use of routing protocols with this kind of network because all nodes "can see" the others.

- The second kind uses also the radio relay system but each node has a smaller range, therefore one node has to use neighboring nodes to reach another node that is not within its transmission range. Then, the intermediate nodes are the routers.

This being said, we can now concentrate on the security aspect of the ad-hoc network. In this paper our main focus is regarding the security of the currently implemented routing algorithms. The focus is mainly on the security of the routing protocols used in the second kind of ad-hoc network described above.

Any routing protocol must encapsulate an essential set of security mechanisms. These are mechanisms that help prevent, detect, and respond to security attacks. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment.

Background

Mobile ad hoc networks are being extensively deployed currently since they provide some features which are difficult or impossible to be emulated by conventional networks. The applications range from the defense sector (sensor nodes in hostile territory) to general transportation (gadgets used to communicate traffic congestion while traveling) to providing useful infrastructure during disaster recovery. Due to the significance attached to the applications of MANET, security in ad hoc networks is a hot research area and already considerable research is done in this field.

Use of wireless links renders an ad-hoc network susceptible to link attacks ranging from passing eavesdropping to active impersonation, message replay and message distortion. Nodes roaming freely in a hostile environment with relatively poor physical protection have non-negligible probability of being compromised. Hence, we need to consider malicious attacks not only from outside but also from within the network from compromised nodes [24]. Eavesdropping might give an attacker access

to secret information thus violating confidentiality. Active attacks could range from deleting data, injecting erroneous messages; impersonate a node etc. thus violating availability, integrity, authentication and non-repudiation.

Most of the security measures surrounding ad-hoc networks in general and their routing solutions are, as yet, incomplete and mostly inefficient. Hence we propose a security framework that is integrated into the routing protocols in the design phase itself as a viable solution to satiate the security needs of the ad hoc networks.

SecurityIssues :

The contemporary routing protocols for ad-hoc networks cope well with dynamically changing topology but are not designed to accommodate defense against malicious attackers. Today's routing algorithms are not able to thwart common security threats. Most of the existing ad hoc routing protocols do not accommodate any security and are highly vulnerable to attacks. [13] discusses threats and attacks against ad hoc routing under several areas of application and suggested solutions that could be used when secure protocols are designed.

Routers exchange network topology informally in order to establish routes between nodes - another

Potential target for malicious attackers who intend to bring down the network. External attackers inject erroneous routing information, replaying old routing information or distort routing information in order to partition a network or overload a network with retransmissions, thereby causing congestion, and hence a denial of service. Internally compromised nodes are harder to detect and correct. Routing information signed by each node will not work since compromised nodes can generate valid signatures using their private keys. Detection of compromised nodes through routing information is also difficult due to the dynamic topology of ad-hoc networks.

In mobile ad-hoc networks, nodes do not rely any routing infrastructure but relay packets Each other Thus communication in mobile ad-hoc networks functions properly only is the participating nodes cooperate in routing and forwarding [19]. However, it may advantageous for individual nodes not to cooperate, for example to save power or to launch security attacks such as denial-of-service. In this paper, we give an overview of potential vulnerabilities and security requirements of mobile ad-hoc networks, and proposed prevention, detection and reaction mechanisms to thwart attacks.

Types of Ad-Hoc Routing Protocols

Basically there are two types of routing protocols:

1. *Proactive Routing Protocols:* Herein the nodes keep updating their routing tables by periodical messages. This can be seen in Optimized Link State Routing Protocol (OLSR) and the Topology Broadcast based on Reverse Path Forwarding Protocol (TBRPF).
2. *Reactive or On Demand Routing Protocols:* Here the routes are created only when they are needed. The application of this protocol can be seen in the Dynamic Source Routing Protocol (DSR) and the Ad-hoc On- demand Distance Vector Routing Protocol (AODV).In today's world the most common ad-hoc protocols are the Ad-hoc On-demand Distance Vector routing protocol and the Destination-Sequenced Distance-Vector routing protocol and the Dynamic Source Routing. All these protocols are quite insecure because attackers can easily obtain information about the network topology.

the network. With all this information more serious attacks can be launched in order to disrupt network operations.

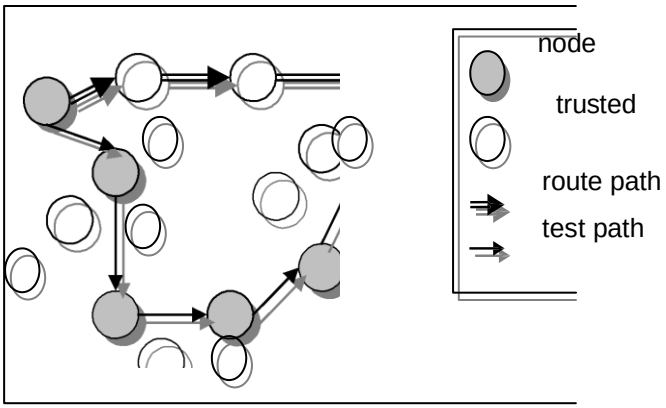

Fig: 2: variation of shortest path route selection between SAR and routing algorithms.

This is because in the AODV and DSR protocols, the route discovery packets are carried in clear text. Thus a malicious node can discover the network structure just by analyzing this kind of packets and may be able to determine the role of each node.

SAR is indeed secure in the way that it does ensure that only nodes having the required trust level will read and reroute the packets being sent. Unfortunately, SAR still leaves a lot of security issues uncovered and still open for attacks such as:

- Nothing is done to prevent intervention of a possibly malicious node from being used for routing, as long as they have the required key

If a malicious node somehow retrieves the required key the protocol has no further security measure to

prevent against the attacker from bringing the entire network to a standstill.

There is excessive encryption and decryption required at each hop. Since we are dealing with mobile environments the extra processing leading to increased power consumption can be a problem.

SAR is intended for the managed-open environment as it requires some sort of key distribution system in order to distribute the trust level keys to the correct devices.

More than one route request packet reaches the destination through different routes. The destination T calculates a MAC covering the route request packets to provide the source with an as diverse topology picture as possible.

The evident failing, however, is that it exposes network infrastructure information to potential attackers. In fact one of the main security issues in SRP is that it has no defense against the "invisible node" attack that simply puts itself (and possibly a large number of other invisible nodes) somewhere along the message path without adding itself to the path, thereby causing potentially big problems as far as routing goes.

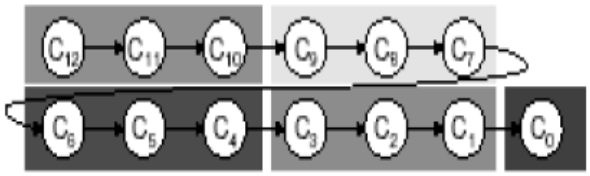

Figure 3: Hash chains in SEAD

To avoid routing loops the source of each routing update message must be authenticated. This protocol requires pair wise shared secret keys or broadcast authentication such as TESLA, HORS or TIK to authenticate neighbors.

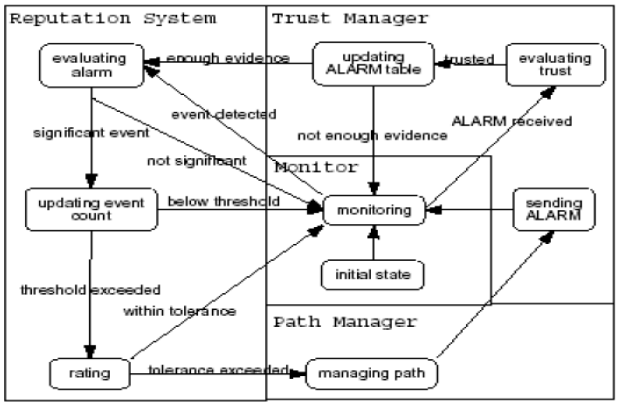

Figure 4: Trust architecture and FMS within each node of a Confidant

1. *The Trust Manager:*

Responsible for calculating trust levels of nodes and dealing with all incoming and outgoing alarm messages.

2. *The Path Manager:*

Manages all path information, i.e. adds, deletes or updates paths according to the feedback it receives from the reputation system

A sample working follows:

When a node forwards a packet, the Watchdog verifies that the neighbor on the path also forwards the packet. This is done by listening to the transmissions of all neighbors. The watchdog then assign positive values to a node that forwards packets successfully and a negative value after a threshold level of misbehavior has been observed.

Figure 5: Operation performed by the Watchdog plug- in

The Path rater uses this knowledge of the misbehaving nodes to choose the network path that is most likely to deliver packets. The decision is taken based on the average of the values obtained by the watchdog about each node in the path. In any reputation-based mechanism, detecting the propagation of positive ratings by colluding nodes is a challenging task. Further, if a node is unable to forward packets either due to overload or low transmission power, detection protocols assume misbehavior in such circumstances, resulting in false positives.

This property offers an advantage over infrastructure-based local area networks that can be exploited by diversity coding.

Besides authentication, confidentiality, integrity, availability, access control, and non repudiation being harder to enforce because of the properties of mobile ad-hoc networks, there are also additional requirements such as location confidentiality, cooperation fairness and the absence of traffic diversion.

Conclusions

Mobile ad-hoc networks have properties that increase their vulnerability to attacks. Unreliable wireless links are vulnerable to jamming and by their inherent broadcast nature facilitate eavesdropping. Constraints in bandwidth, computing power, and battery power in mobile devices can lead to application-specific trade- offs between security and resource consumption of the device. Mobility/Dynamics make it hard to detect behavior anomalies such as advertising bogus routes, because routes in this environment change frequently. Self-organization is a key property of ad-hoc networks. They cannot rely on central authorities and infrastructures, e.g. for key management. Latency is inherently increased in wireless multi-hop networks, rendering message exchange for security more expensive. Multiple paths are likely to be available.

References

1. J.-P. Hubaux, L. Buttyan, and S. Capkun,
The quest for security in mobile ad hoc networks," in The 2nd ACM Symposium on Mobile Ad Hoc Networking and Computing, October 2001.

2. L. Zhou and Z. Haas, Securing ad hoc networks," IEEE Network Magazine, vol. 13, November/December 1999.

3. Manel Guerrero Zapata. Secure Ad hoc On-Demand Distance Vector (SAODV) Routing INTERNET-DRAFT draft-guerrero-manet-saodv-
00.txt, August 2002. First published in the IETF MANET Mailing List (October 8th 2001).

4 Bridget Dahill, Brian Neil Levine,
Elizabeth Royer, Clay Shields. A Secure Routing Protocol for Ad Hoc Networks In

Proceedings of the 10 Conference on Network Protocols (ICNP), November 2002.

5 S. Yi, P. Naldurg, and R. Kravets Security-Aware Ad hoc Routing for Wireless Networks The Second ACM Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc'01), 2001.(another version Security-Aware Ad Hoc Routing Protocol for Wireless Networks, Report, August, 2001)

6 Panagiotis Papadimitratos and Zygmunt J. Haas Secure Routing for Mobile Ad hoc Networks SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.

7 Yih-Chun Hu, David B. Johnson, and Adrian Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3-13, IEEE, Calicoon, NY, June 2002.

8 Baruch Awerbuch, David Holmer, Cristina Nita-Rotaru and Herbert Rubens An On-Demand Secure Routing Protocol Resilent to Byzantine Failures In ACM Workshop on Wireless Security (WiSe), Atlanta, Georgia, September 28 2002

9 Pietro Michiardi, Refik Molva Core: A Collaborative REputation mechanism to enforrce node cooperation in Mobile Ad Hoc Networks in Communication and Multimedia Security 2002 Conference

10 Sergio Marti and T. J. Giuli and Kevin Lai and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. Mobile Computing and Networking (2000):